PCT/IB 04/2279

1

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03291741.1

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

REC'D 02 AUG 2004
WIPO PCT

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03291741.1
Demande no:

Anmeldetag:
Date of filing: 15.07.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Schlumberger Systèmes
50, avenue Jean Jaurès
92120 Montrouge
FRANCE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Concealed electrical connection between security feature and IC

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06K19/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

Concealed electrical connection between security feature and IC

All smart cards bodies.

Several security features are available on the market, like holograms, MLI, CLI, photos, laser engraving... that are placed directly on the card body at the manufacturing stage or being introduced at the final personalization stage by clients.

The problem lies in the integrity and the security of the card in case of IC OR aspect features fraud; Very few features are really secured since they can be simulated, hoaxed or counterfeited very easily.
The most common type of card physical attack is peeling or modifying at least one layer to change printed or engraved information. Photos printed on a card (like on a driving license, passport etc...) or IC alteration are usually the first targets of physical attacks.

An irreversible system should be implemented to ensure the non-functionality of the card if any fraud attacks are applied to any card layer containing security features, which also works as a tamper-proof feature.

An invisible customizable electrically conductive material circuit is integrated on the card critical layers and connected to the IC before or after security features introduction. Basically it works as an interrupter switch that permanently deactivates the chip in case of any fraud since the circuit will be broken and /or the electrical properties such as impedance or electrical resistance will be modified.

The invisible circuit is connected to the IC (contact module, contactless module, or hybrid module) or chip by any mean. When the card communicates with a reader (contact or contactless) the invisible circuit integrity and/or electrical properties are checked.

See figure 1.

In the following example, the picture and the other security feature are present on the same layer, on top of which is located the invisible printed conductive circuit. The latter is connected to an Integrated Circuit module. This constitutes the so-called security layer that is integrated into the card structure.

The use of inks is easy since they can be printed (offset or screen-printed for instance) right on the security feature to be protected (photo, hologram, logo...) before the layer is inserted into the card structure. This also enables the card manufacturer to customize circuit shapes, which leads to modifying some properties of the circuit like its electrical resistance, impedance or behavior when exposed to contact-less readers (circuit can act as a contactless antenna).

- **Advantages**
  - Less security features needed to protect the card or IC i.e. less manufacturing cost
  - Uses classic manufacturing processes
  - Cheaper than most security features like holograms or laser photo engraving
  - Covers both physical attacks like layer peeling and IC exchange at once.
  - The circuit is invisible to human eye in daylight, which makes it difficult to detect when card is visually inspected in daylight.
  - Customizable: every XX batch, design (circuit properties) can be modified.
  - Irreversible system.

Claim

1. Card wherein the card comprises a chip.

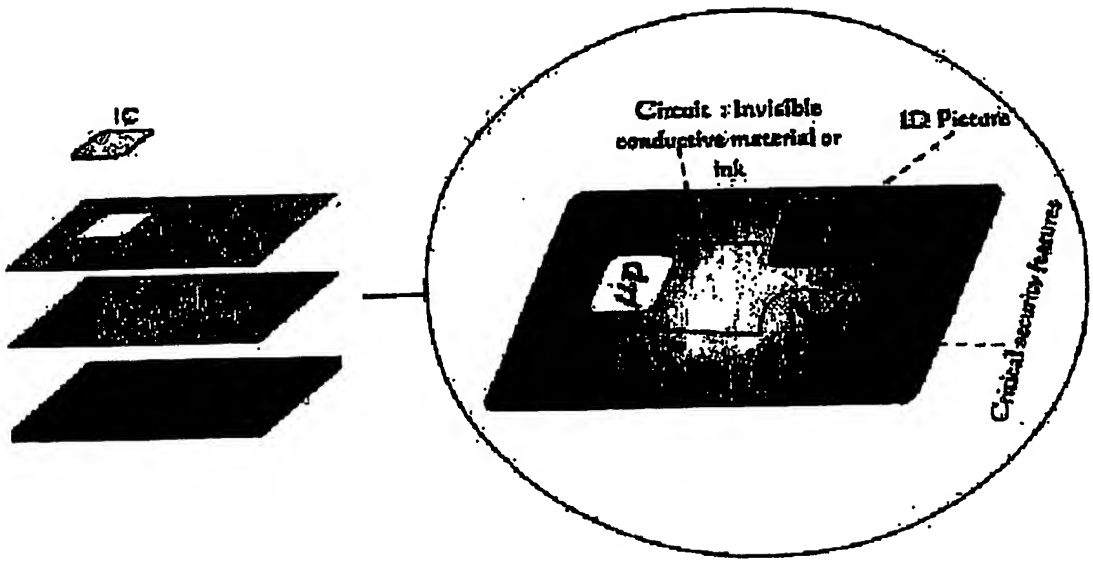

Figure 1